IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ANATOLI BELOV, IRINA BELOVA, and ERYN KAPLAN, individually and as a natural guardian of H.M.K., a minor child, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Case No. 23-8583 **JURY TRIAL DEMANDED**

Plaintiffs Anatoli Belov, Irina Belova and Eryn Kaplan, individually and as a natural guardian of H.M.K., a minor child, bring this class action lawsuit in their individual capacities and on behalf of all others similarly situated against Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJ&A") (collectively, "Defendants"). Plaintiffs' allegations are based upon personal knowledge as to themselves and their own acts, and upon information and good faith belief as to all other matters based on the investigation conducted by Plaintiffs' attorneys.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and a data breach that began as early as March 27, 2023 and lasted until May 2, 2023, where third-party criminals retrieved and exfiltrated personal data from PJ&A's network resulting in unauthorized access to highly sensitive medical and personal data of Plaintiffs and of approximately 3.9 million Class

Members ("Data Breach").[1]

2. This is one of the worst medical data breaches in recent years.

3. Almost 9 million victims in total, including Plaintiffs, were affected by the Data Breach.[2]

4. After learning of the Data Breach, PJ&A waited ***more than two and a half*** **months** to notify affected customers, including Northwell, the largest healthcare system in New York State.[3]

5. Defendants Northwell and PJ&A did not begin notifying Plaintiffs until ***almost five months*** after the Data Breach was discovered.[4]

6. According to the Data Breach notice submitted to the California Attorney General, information compromised in the Data Breach represents a gold mine for data thieves and includes personally identifying information ("PII") and protected health information ("PHI") such as names, date of birth, address, medical record number, hospital account number, admission diagnoses, and dates and times of service as well as Social Security numbers and insurance information and clinical information from medical transportation files, such as laboratory and diagnostic testing results, medications, name of treatment facility and name of healthcare providers (collectively, "PII" and "PHI" is "Private Information").[5]

---

[1] *See* https://techcrunch.com/2023/11/15/9-million-patients-had-data-stolen-after-us-medical-transcription-firm-hacked/ (last visited Nov. 16, 2023).

[2] *Id.*

[3] *See* Plaintiff Eryn Kaplan's Notice of the Data Breach, attached hereto as Exhibit A.

[4] *Id.*

[5] *See* Data Breach Notice, https://oag.ca.gov/ecrime/databreach/reports/sb24-576068 (last visited

7. Plaintiffs bring this class action lawsuit individually and on behalf of those similarly situated to address Defendants' inadequate safeguarding of Plaintiffs' and Class Members' Private Information that Defendants collected and maintained.

8. Defendants maintained the Private Information collected from Plaintiffs and Class Members in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendants' computer systems and networks in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure Private Information from those risks left that Private Information in a vulnerable condition.

9. Indeed, this was not the first data breach at Northwell this year. Northwell was affected by an exploitation earlier this year of a zero-day vulnerability in Progress Software's MOVEit secure file transfer software.[6]

10. In addition, PJ&A Defendant and its employees failed to properly monitor the computer network and IT systems that housed the Private Information. PJ&A Defendant failed to timely detect and report the Data Breach, and to timely notify affected consumers, including Plaintiffs and Class Members, which made Plaintiffs and Class Members vulnerable to identity theft without any warnings that they needed to act to prevent unauthorized use of their Private

Nov. 15, 2023).

[6] *See* https://www.northwell.edu/ (providing a link to https://www.nuance.com/moveit-support.html (last visited Nov. 15, 2023)); *see also* https://www.govinfosecurity.com/medical-transcribers-hack-breach-affects-at-least-9-million-a-23597#:~:text=Northwell%20Health's%20statement%20about%20the,affected%20by%20the%20PJ%26A%20hack.(last visited Nov. 15, 2023).

Information.

11. In failing to adequately protect Plaintiffs' and the Class Members' Private Information, failing to adequately notify them about the Data Breach, and obfuscating the nature of the Data Breach, Defendants violated state and federal law and harmed millions of their consumers.

12. Plaintiffs and Class Members are victims of Defendants' negligence and inadequate cybersecurity measures. Specifically, Plaintiffs and Class Members trusted Defendants with their Private Information. But Defendants betrayed that trust, including by failing to properly use up-to-date security practices and measures to prevent the Data Breach, and the exfiltration and theft of Plaintiffs' and Class Members' sensitive Private Information.

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial accounts and taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' names to obtain medical services, using Plaintiffs' and Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining driver's licenses in Plaintiffs' and Class Members' names, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiffs and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiffs and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses and anxiety over the misuse of their Private Information.

15. Even those Plaintiffs and Class Members who have yet to experience identity theft

have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy and/or additional damages as described below.

16. Indeed, Defendants, themselves, encourage Plaintiffs and Class Members to spend time dealing with the Data Breach. In announcing the Data Breach, Defendants have encouraged Plaintiffs and Class Members to carry out a number of tasks, including to regularly review their financial accounts and report any suspicious or unrecognized activity immediately for the next 12 to 24 months and to review statements from healthcare providers.[7]

17. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct; these injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) compromise and disclosure of Private Information and identities, (iv) diminution of value of their Private Information, (iv) statutory damages and (v) the continued and ongoing risk to their Private Information.[8]

18. Accordingly, Plaintiffs bring this action against Defendants seeking redress for their unlawful conduct and asserting claims for: (i) negligence; (ii) breach of contract; (iii) unjust

[7] *See* PJ&A's template Data Breach Notice, https://oag.ca.gov/ecrime/databreach/reports/sb24-576068 (last visited Nov. 15, 2023).

[8] The exposed Private Information of Plaintiffs and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties can often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

enrichment; (iv) breach of fiduciary duty; (v) breach of confidence; (vi) invasion of privacy; (vii) bailment and (viii) declaratory and injunctive relief, as well as various state statutory claims. Through these claims, Plaintiffs seek damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems, future annual audits and adequate credit monitoring services funded by Defendants.

PARTIES

19. Plaintiff Anatoli Belov is a natural person residing in Westchester County in the state of New York, where he intends to remain.

20. Plaintiff Irina Belova is a natural person residing in Westchester County in the state of New York, where she intends to remain.

21. Plaintiffs H.M.K. and Eryn Kaplan, individually and as a natural guardian of H.M.K., a minor child, are natural persons residing in Nassau County in the State of New York, where they intend to remain.

22. Defendant Northwell is a registered non-profit entity with its headquarters and principal place of business at 2000 Marcus Ave, North New Hyde Park, NY 11042.

23. Defendant PJ&A is a domestic corporation incorporated in Nevada, with its principal place of business located at 1489 W. Warm Springs, Suite 110, Henderson, NV 89012.

24. As health care providers and transportation services that transmit health information in electronic form in connection with covered transactions, Defendants are covered entities under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 ("HIPAA").

JURISDICTION & VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331

because it arises under the laws of the United States, and under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

26. This Court has personal jurisdiction over Defendant Northwell because its principal place of business is in this District and a substantial portion of the acts and omissions giving rise to Plaintiffs' and Class Members' claims occurred in and emanated from this District.

27. This Court has personal jurisdiction over Defendant PJ&A because PJ&A intentionally and purposefully availed itself of this jurisdiction by choosing to do business in the state of New York and a substantial portion of the acts and omissions giving rise to Plaintiffs' and Class Members' claims occurred in and emanated from this District.

28. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant Northwell's principal place of business is in this District, and a substantial portion of Defendant Northwell's and Defendant PJ&A's events, acts and omissions giving rise to Plaintiffs' claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendants' Business

29. Northwell was founded in 1997 and has expanded since then to become New York's largest private employer and health care provider, with 21 hospitals and about 900 outpatient facilities.[9]

[9] *See* https://www.northwell.edu/sites/northwell.edu/files/d7/ShapingTheFutureOfHealthcare.pdf; https://www.northwell.edu/sites/northwell.edu/files/2023-03/we-are-northwell-fact-sheet-03-06-2023.pdf (last visited Nov. 15, 2023).

30. Northwell's clinical enterprise consists of five tertiary hospitals—Lenox Hill Hospital, Long Island Jewish Medical Center, North Shore University Hospital, South Shore University Hospital, Staten Island University Hospital, five specialty care hospitals and eleven community hospitals.[10]

31. As the owner and operator of these medical centers and entities, Northwell offers a wide range of services, from primary and urgent care to cancer treatment, cardiac and kidney transplants, heart and vascular, orthopedics and neurology.[11]

32. According to the Cyber Incident Notice posted on Northwell's website, Northwell uses various third-party vendors to conduct its healthcare operations.

33. One such vendor is Defendant PJ&A, which provides medical transcription services for Northwell's patients.[12]

34. PJ&A has over thirty years of history and experience in healthcare operations.[13]

35. To obtain healthcare and related clinical laboratory and medical transportation services, patients like Plaintiffs and Class Members, must provide their doctors, medical professionals and/or Defendants directly with highly sensitive Private Information. As part of their businesses, Defendants then compile, store and maintain the Private Information they receive from

---

[10] *See* https://www.northwell.edu/sites/northwell.edu/files/2023-07/we-are-northwell-fact-sheet-july-2023.pdf (last visited Nov. 15, 2023).

[11] *See* https://www.northwell.edu/doctors-and-care/locations?type=clinical-departments (last visited Nov. 15, 2023).

[12] *See* https://www.northwell.edu/ (providing a link to https://www.pjats.com/downloads/Notice.pdf. (last visited Nov. 15, 2023)).

[13] *See* https://www.pjats.com/ (last visited Nov. 15, 2023).

patients and healthcare professionals who utilize Defendants' services.

36. Northwell hired PJ&A, a medical technology company, for the transcription and dictation of Northwell's patient data, including the storage of Plaintiff's and Class members' PII. Like millions of New Yorkers, Plaintiffs, and the Class Members, provided their PII to Northwell for health purposes, including receiving medical services. In undertaking this responsibility, Northwell was obligated to only hire vendors who maintain adequate security measures.

37. As a vendor to Northwell, Defendant PJ&A is a "business associate" under HIPAA and would have been required to enter into a Business Associate Agreement ("BAA") with Northwell, which establishes permitted and required uses of PHI, provides obligations for PJ&A to safeguard the information and to report and uses or disclosures not provided for in the BAA, and requires termination of the BAA if there is a material violation.[14]

38. Defendants have created and maintain massive repositories of Private Information: a particularly lucrative target for data thieves looking to obtain, misuse or sell patient data.

39. On information and belief, in the ordinary course of their business of providing medical services, Defendants maintain the Private Information of their clients and/or patients, including but not limited to:

a. Name, address, phone number and email address;

b. Date of birth;

c. Demographic information;

d. Social Security number;

[14] *See* Northwell's HIPAA Business Associate Policy, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.northwell.edu/sites/northwell.edu/files/2020-07/HIPAA-business-associate-policy.pdf (last visited Nov. 17, 2023).

e. Financial and/or payment information;

f. Information relating to individual medical history;

g. Information concerning an individual's doctor, nurse or other medical providers;

h. Health insurance information;

i. Clinical testing information and results;

j. Other information that Defendants may deem necessary to provide services and care.

40. Additionally, Defendants may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends and/or family members.

41. Because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to patients and other individuals, Defendants, upon information and belief, promises to, among other things: keep PHI private; comply with healthcare industry standards related to data security and Private Information, including HIPAA; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

42. As HIPAA-covered business entities (*see infra*), Defendants are required to implement adequate safeguards to prevent the unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

43. According to Northwell's website, "patients are our number one priority and we believe that patient privacy is an integral part of the health care we provide you."[15] The website continues, "[t]o ensure the development of a lasting bond of trust with our patients, we have many safeguards to protect the privacy and security of your personal information…We also have many policies in place to protect the privacy and security of your personal information and our employees are educated from the moment they are hired and continually after, to respect and protect patient privacy."[16]

44. However, Defendants did not maintain adequate security to protect their systems from infiltration by cybercriminals, and they waited nearly ***five months*** to publicly disclose the Data Breach.

45. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

B. The Data Breach and Notice Letter

46. According to the Notice Letter PJ&A provided to Plaintiffs and Class Members, PJ&A was subject to a cyber-attack where unauthorized parties accessed PJ&A's systems for more than a month between March 27, 2023 and May 2, 2023, and that unauthorized access to personal health information of Northwell patients specifically occurred between April 7, 2023 and April 19, 2023.

---

[15] *See* https://www.northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy (last visited Nov. 17, 2023).

[16] *Id.*

47. As a result of the attack on PJ&A's systems, Private Information from several healthcare systems, including Northwell's, was stolen by cyber thieves.

48. PJ&A became aware of the data security incident on its network only on May 2, 2023. In response, according to the Notice Letter, PJ&A allegedly "launched an internal investigation and retained an external cybersecurity vendor to assist with the investigation, contain the threat and further secure its systems."[17]

49. The Notice – and Defendants' response to the Data Breach – are glaringly deficient.

50. After discovering the Data Breach, it took PJ&A an entire three weeks to "preliminarily determine[]" that an unauthorized third party had likely accessed Northwell's patient data, on May 22, 2023.[18]

51. It then took PJ&A more than four months to "confirm[] the scope of the Northwell data impacted."[19]

52. The breach notice does not state who this "unauthorized third party" was or whether a ransomware demand was made to or paid by PJ&A.[20]

53. PJ&A waited nearly ***five months*** from the date it learned of the Data Breach and the highly sensitive nature of the Private Information impacted to publicly disclose the Data Breach and notify some of affected individuals.

[17] *See* template Notice, at note 7.

[18] *See* Exhibit A.

[19] *Id.*

[20] *See* template Notice, at note 7.

54. Northwell's Notice of Privacy Practices states, "You have a right to be notified in the event of a breach of the privacy of your unsecured protected health information by Northwell Health or its business associates."[21] The Notice of Privacy Practices promises patients that they "will be notified as soon as reasonably possible, but no later than 60 days following our discovery of the breach."[22]

55. Northwell learned of the breach on or about July 21, 2023, but Defendants did not disclose the breach to Northwell patients until early November, 2023, or over three months later.

56. In fact, it appears that the data of about ***four million*** patients remained unaccounted for as of two days ago, on November 15, 2023.[23]

57. Defendants' failure to promptly notify Plaintiffs and Class Members that their PII and PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class Members will suffer indefinitely from the substantial and concrete risk that their identifies will be (or already have been) stolen and misappropriated.

58. In the aftermath of the Data Breach, PJ&A purports to "continue to take, appropriate steps to help prevent incidents of this nature from occurring in the future, including by further enhancing our security systems."[24]

---

[21] *See* https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf

[22] *Id.*

[23] *See* note 1.

[24] *See* note 7.

59. In other words, Defendant PJ&A admits its security systems are inadequate and that additional security was required to protect highly sensitive personal and health information entrusted to it, but there is no indication whether the unspecified "appropriate" steps will adequately protect Plaintiffs' and Class Members' Private Information going forward.[25]

60. In fact, some of PJ&A's customers have the same doubts about PJ&A's ability to protect their patients' highly sensitive data. Cook County Health, a PJ&A customer that had up to 1.2 million patients' data stolen in the Data Breach, reported that it stopped sharing data with PJ&A when it was notified about the Data Breach on July 26, 2023 and has since terminated its business relationship with Defendant PJ&A.[26]

61. Upon information and belief, Defendant Northwell has not stopped sharing its patients' highly sensitive data with PJ&A and has not terminated its relationship with PJ&A, despite the apparent risks of continuing to provide such incredibly sensitive data to Defendant PJ&A.

62. Further, while Defendants arranged to have credit/identity monitoring services for Plaintiffs and Class Members, they have done so for only 12 months, an entirely inadequate amount of time given that this Private Information is now in the hands of cyber criminals who can use it several years from now for a variety of crimes.

63. Defendants recognize these long-term risks to Plaintiffs and Class Members, as they themselves recommend that Plaintiffs and Class Members "should carefully monitor [their]

[25] *See* template Notice, at note 7.

[26] *See* https://www.hipaajournal.com/cook-county-health-1-2-million-breach-business-associate/ (last visited Nov 17, 2023).

accounts for the next 12 to 24 months and report any suspected incidents of fraud to the relevant financial institution."[27]

64. Defendants declare that they "are committed to maintaining the privacy and security of [Plaintiffs' and Class Members'] information and take this incident very seriously."[28]

65. Yet, despite the ongoing and long-term risks of financial and medical fraud and identity theft for Plaintiffs and Class Members, instead of automatically signing up Plaintiffs and Class Members for identity protection services, Defendants place the burden of signing up for these services squarely on the victims of their negligence.

66. Defendants' systems hacked by cyber thieves contained Plaintiffs' and Class Members' Private Information that was accessible, unencrypted, unprotected and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

67. As HIPAA-covered business entities that collect, create and maintain significant volumes of Private Information, the targeted attack was a foreseeable risk which Defendants Northwell and PJ&A were aware of, and that Defendants knew they had a duty to guard against.

68. This is particularly true because the targeted attack was a ransomware attack. It is well-known that healthcare businesses such as Defendants, which collect and store the confidential and sensitive PII/PHI of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

[27] *See* Exhibit A.

[28] *See id.*

69. In this case, PJ&A has acknowledged that the cyberattack exposed data of nearly nine million patients, of which over 30% were Northwell patients.[29]

70. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of Northwell's patients, like Plaintiffs and Class Members.

71. Defendants had obligations created by HIPAA, contract, industry standards, common law and their own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

72. Plaintiffs and Class Members provided their Private Information to Defendants, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

73. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants Northwell and PJ&A assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

74. Due to PJ&A's and Northwell's inadequate security measures and PJ&A's delayed notice to victims, Plaintiffs and Class Members now face a present, immediate and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

C. Defendants are Covered Entities Subject to HIPAA.

[29] *See* https://www.bleepingcomputer.com/news/security/pj-and-a-says-cyberattack-exposed-data-of-nearly-9-million-patients/amp/ (last visited Nov. 16, 2023).

75. Defendants had duties to ensure that all information they collected and stored was secure, and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiffs' and Class Members' Private Information.

76. As a medical transportation provider, Defendant PJ&A is a covered entity.

77. As a healthcare provider, Defendant Northwell is a covered entity.

78. Defendants are both HIPAA covered entities that provide services to patients and/or healthcare and medical service providers. As a regular and necessary part of their businesses, Defendants collect the highly sensitive Private Information of their clients and/or patients.

79. As covered entities under HIPAA, Defendants are required under federal and state law to maintain the strictest confidentiality of their clients and/or patients' Private Information that they acquire, receive and collect, and Defendants are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

D. Defendants' Conduct Violates HIPAA Obligations to Safeguard Private Information.

80. Because Defendants are covered by HIPAA (*see* 45 C.F.R. § 160.102), they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

81. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[30] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[30] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

82. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

83. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

84. HIPAA requires that Defendants implement appropriate safeguards for this information.

85. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

86. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

87. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates, like Defendants, to provide notification following a

breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable or indecipherable to unauthorized persons—i.e. non-encrypted data—to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[31]

88. HIPAA requires covered entities to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

89. HIPAA requires covered entities to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

90. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[32] The list of resources includes a link to guidelines set by the National Institute of

[31] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/forprofessionals/breach-notification/index.html (emphasis added).

[32] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[33]

91. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported." The four-factor risk assessment focuses on:

(1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and,

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[34]

92. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own Privacy Practices. Indeed, Defendants failed to:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiffs' and Class Members' Private Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

---

[33] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

[34] 78 Fed. Reg. 5641-46; see also 45 C.F.R. § 164.304.

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h) Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i) Conduct the Four Factor Risk Analysis following the Breach;

j) Properly send notice to Plaintiffs and Class Members pursuant to 45 C.F.R. §§ 164.400- 414;

k) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

l) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

93. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

94. Defendants failed to comply with their duties under HIPAA and their own privacy

policies despite being aware of the risks associated with the unauthorized access of Plaintiffs' and Class Members' Private Information.

95. Defendants' Data Breach resulted from a combination of insufficiencies that indicate that Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards.

E. Defendants had Legal and Equitable Duties to Safeguard Plaintiffs' and Class Members' Private Information.

96. Due to the nature of Defendants' businesses, which include providing a range of medical transportation and clinical medical services for patients and services for Defendants' healthcare and medical clients, including storing and maintaining electronic health records, Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information that they know and understand to be sensitive and confidential.

97. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

98. Plaintiffs and Class Members are or were patients whose medical records and Private Information were maintained by, or who received health-related or other services from Northwell and/or PJ&A and directly or indirectly entrusted Defendants with their Private Information.

99. Plaintiffs and Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes

and to prevent the unauthorized disclosures of the Private Information. Plaintiffs and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep that Private Information confidential.

100. As described throughout this Complaint, Defendants Northwell and PJ&A did not reasonably protect, secure or store Plaintiffs' and Class Members' Private Information prior to, during or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendants maintained. Consequently, cybercriminals circumvented Defendants' security measures, resulting in a significant data breach.

F. The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

101. As HIPAA-covered entities handling medical patient data, Defendants Northwell's and PJ&A's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

102. At all relevant times, Defendants knew, or should have known, that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that Defendants should have anticipated and guarded against.

103. Importantly, this is not the first data breach that Defendant Northwell experienced this year.[35]

[35] *See* https://www.northwell.edu/ (providing a link to https://www.nuance.com/moveit-support.html (last visited Nov. 15, 2023)).

104. By July 10, 2023, Progress Software notified Northwell patients that due to a vulnerability in its MOVEit secure file transfer software, Northwell's patients' PII and PHI were hacked and accessed by cybercriminals.[36]

105. Moreover, in light of high-profile data breaches at other health care providers and vendors, Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

106. These data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to harden their systems and engage in better, more comprehensive cybersecurity practices.

107. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[37]

108. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[38]

---

[36] *Id.*

[37] *2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (last visited May. 7, 2023).

[38] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), *available at*: https://healthitsecurity.com/news/health-

109. Indeed, cyberattacks against the healthcare industry have been common for over eleven years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that "the increasing sophistication of cybercriminals will no doubt lead to an escalation in cybercrime."[39]

110. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[40] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[41] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[42]

111. Cyberattacks on medical systems, like Defendants', have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of,

---

sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Nov. 15, 2023).

[39] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited Nov. 15, 2023).

[40] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited Nov. 15, 2023).

[41] *Id.*

[42] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Nov. 15, 2023).

and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[43]

112. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[44]

113. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[45] In this case, Defendants PJ&A and Northwell stored the records of *millions* of patients.

114. Private Information, like that stolen from Defendants, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web

---

[43] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Nov. 15, 2023).

[44] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records (last visited Nov. 15, 2023).

[45] *See id.*

sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[46]

115. Indeed, cybercriminals are also monetizing encrypted data by saving it until decryption methods are developed, at which point the data will be combined with the rest of the "fullz." This practice is well-known among entities actively monitoring for such risks, as Defendants should reasonably have been doing.

116. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

117. Defendants were on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[47]

118. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some

[46] *See id.*

[47] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited Nov. 15, 2023).

> kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[48]

119. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

120. HHS and OCR urge the encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[49]

121. As HIPAA-covered entities, Defendants should have known about their data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

G. Defendants Fail to Comply with FTC Guidelines.

122. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

---

[48] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals. (last visited Nov. 15, 2023).

[49] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops (last visited Nov. 15, 2023).

123. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities and implement policies to correct any security problems.[50]

124. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[51]

125. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

126. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

[50] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 15, 2023).

[51] *Id.*

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

127. Defendants failed to properly implement basic data security practices.

128. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

129. Defendants were at all times fully aware of their obligation to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

H. Defendants Fail to Comply with Industry Standards.

130. As shown above, experts studying cybersecurity routinely identify healthcare providers, partners and vendors as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

131. Several best practices have been identified that, at a minimum, should be implemented by healthcare service providers like Defendants, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limitations on which employees can access sensitive data.

132. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

133. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

134. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and, ultimately, causing the Data Breach.

135. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with industry safeguards.

I. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

136. Cyberattacks and data breaches at healthcare companies like Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

137. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[52]

138. Researchers have further found that at medical service providers that experienced

[52] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Nov. 15, 2023).

a data security incident, the incident was associated with a deterioration in timeliness and patient outcomes, generally.[53]

139. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[54]

140. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate the pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

---

[53] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Nov. 15, 2023).

[54] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Nov. 15, 2023).

141. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[55]

142. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

143. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

144. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[56]

145. Its value is axiomatic, considering the value of "big data" in corporate America and

[55] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Nov. 15, 2023).

[56] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (last visited Nov. 15, 2023).

the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

146. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

147. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. *See* GAO Report, at p. 29.

148. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

149. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

150. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of their children for many years to come.

151. Private Information can sell for as much as $363 per record according to the Infosec Institute.[57] Private Information is particularly valuable because criminals can use it to target

[57] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Nov. 15, 2023).

victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

152. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[58] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits or apply for a job using a false identity.[59] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

153. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

154. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[60]

---

[58] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 15, 2023).

[59] *Id*.

[60] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Nov. 15, 2023).

155. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[61]

156. Medical information is especially valuable to identity thieves.

157. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[62]

158. Drug manufacturers, medical device manufacturers, clinical laboratories, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

159. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

160. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were on notice of the

[61] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 15, 2023).

[62] *See* FTC, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Nov. 15, 2023).

substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

161. Defendants placed themselves in a position where they owed a duty to Plaintiffs and Class Members by virtue of the sensitivity of the data that they collected. Indeed, because of Defendants, Plaintiffs and Class Members were placed in a worse position than they would have been had Defendants not collected and maintained their data. Defendants knew the risk that they created and, accordingly, were in the best position to protect Plaintiffs and Class Members by virtue of the special relationship that they created with them.

J. Defendants' Data Breach.

162. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic

information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

163. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class

Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems for multiple days which contained unsecured and unencrypted Private Information.

164. Accordingly, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants.

K. Plaintiffs' and Class Members' Damages as a Result of Defendants' Data Breach.

165. Plaintiffs provided their Private Information to Defendants either directly or via their healthcare providers as part of the process of obtaining medical services provided by Defendants, and Plaintiffs trusted that this information would be safeguarded according to state and federal law.

166. Plaintiffs are very careful with their Private Information. They store any documents containing their Private Information in a safe and secure location or destroy the documents. Plaintiffs have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiffs diligently choose unique usernames and passwords for their various online accounts.

167. As a result of the Data Breach, Plaintiffs each made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring their credit.

168. Plaintiffs were each forced to spend multiple hours attempting to mitigate the effects of the Data Breach. They will continue to spend valuable time they otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

169. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Yet, to date, Defendants have only offered an unidentified subset of victims of the Data Breach with limited subscriptions, for an extremely short duration, to fraud and identity monitoring services. Defendants have done nothing to compensate Plaintiffs or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiffs and Class Members as a result of the Data Breach.

170. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

171. Plaintiffs' and Class Members' names, dates of birth, and several categories of highly sensitive medical information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendants' computer system(s).

172. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

173. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, canceling credit and debit cards and monitoring accounts for fraudulent activity.

174. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

175. As a direct and proximate result of Defendants' conduct, Plaintiffs' and Class

Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

176. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

177. Plaintiffs and Class Members face a substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

178. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

179. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

180. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

181. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not

get what they paid for and agreed to.

182. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

183. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts and credit reports for unauthorized activity for years to come.

184. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

185. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be

disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

186. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Anatoli Belov

187. Plaintiff Anatoli Belov is an adult individual and citizen of New York.

188. Plaintiff Belov has been a patient at Northwell s since approximately 2020,.

189. Northwell and PJ&A collected and stored Plaintiff Belov's PHI and PII as a condition of providing Plaintiff with medical care.

190. Plaintiff Belov received a letter from PJ&A notifying him of the Data Breach and of the unauthorized exposure of his PHI and PII.

191. Plaintiff Belov values his privacy and makes every effort to keep his personal information private.

192. Plaintiff Belov faces a substantial risk of being targeted in the future for phishing, data intrusion and other illegal schemes based on his PHI and PII, as potential fraudsters will use exposed information to target Plaintiff more effectively.

193. As a result of the Data Breach, Plaintiff Belov has had to spend several hours monitoring his accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

194. Plaintiff Belov is now forced to live with the anxiety that his PHI and PII, including

sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Belov to embarrassment and depriving him of any right to privacy whatsoever.

195. As a result of Defendants' conduct, Plaintiff Belov has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of his private and confidential personal information, the loss of the benefit of his contractual bargain with Defendants, emotional distress and other economic and non-economic harm.

196. Plaintiff Belov remains at a substantial and imminent risk of future harm given the highly sensitive nature of the information stolen. Plaintiff Belov faces a substantial risk of out-of-pocket fraud losses, such as loans opened in his name, medical services billed in his name, tax return fraud, utility bills opened in his name, credit card fraud and similar identity theft.

197. Plaintiff Belov will now be forced to expend additional time to freeze credit, review credit reports and monitor financial accounts and medical records for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

Plaintiff Irina Belova

198. Plaintiff Irina Belova is an adult individual and citizen of New York.

199. Plaintiff Belova has been a patient at Northwell s since approximately 2013.

200. Northwell and PJ&A collected and stored Plaintiff Belova's PHI and PII as a condition of providing Plaintiff with medical care.

201. Plaintiff Belova received a letter from PJ&A notifying her of the Data Breach and of the unauthorized exposure of her PHI and PII.

202. Plaintiff Belova values her privacy and makes every effort to keep her personal

information private.

203. Plaintiff Belova faces a substantial risk of being targeted in the future for phishing, data intrusion and other illegal schemes based on her PHI and PII, as potential fraudsters will use exposed information to target Plaintiff more effectively.

204. As a result of the Data Breach, Plaintiff Belova has had to spend several hours monitoring her accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

205. Plaintiff Belova is now forced to live with the anxiety that her PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiff Belova to embarrassment and depriving her of any right to privacy whatsoever.

206. As a result of Defendants' conduct, Plaintiff Belova has suffered actual ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of her private and confidential personal information, the loss of the benefit of her contractual bargain with Defendants, emotional distress and other economic and non-economic harm.

207. Plaintiff Belova remains at a substantial and imminent risk of future harm given the highly sensitive nature of the information stolen. Plaintiff Belova faces a substantial risk of out-of-pocket fraud losses, such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud and similar identity theft.

208. Plaintiff Belova will now be forced to expend additional time to freeze credit, review credit reports and monitor financial accounts and medical records for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

Plaintiffs Eryn Kaplan and her minor child H.M.K. (the "Kaplan Plaintiffs")

209. Plaintiff Eryn Kaplan is an adult individual and citizen of New York.

210. Plaintiff Eryn Kaplan has been a patient of Northwell for at least ten years.

211. Plaintiff H.M.K is a minor child and citizen of New York represented by his or her adult guardian, Plaintiff Kaplan, in this action.

212. Northwell and PJ&A collected and stored Plaintiffs' PHI and PII as a condition of providing Plaintiffs with medical care.

213. Kaplan Plaintiffs received two separate letters from PJ&A notifying them of the Data Breach and of the unauthorized exposure of their PHI and PII.

214. Kaplan Plaintiffs value their privacy and make every effort to keep their personal information private.

215. Plaintiff Eryn Kaplan monitors her minor child H.M.K.'s online activity on a regular basis.

216. Kaplan Plaintiffs face a substantial risk of being targeted in the future for phishing, data intrusion and other illegal schemes based on their PHI and PII, as potential fraudsters will use exposed information to target Plaintiffs more effectively.

217. As a result of the Data Breach, Plaintiff Eryn Kaplan has had to spend several hours monitoring her and her child's accounts to detect suspicious and fraudulent activity to mitigate against potential harm.

218. Kaplan Plaintiffs are now forced to live with the anxiety that their PHI and PII, including sensitive medical information, may be disclosed to the entire world, thereby subjecting Plaintiffs to embarrassment and depriving them of any right to privacy whatsoever.

219. As a result of Defendants' conduct, Kaplan Plaintiffs have suffered actual

ascertainable damages including, without limitation, time and expenses related to monitoring financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, a diminution in the value of their private and confidential personal information, the loss of the benefit of their contractual bargain with Defendants, emotional distress and other economic and non-economic harm.

220. Kaplan Plaintiffs remain at a substantial and imminent risk of future harm given the highly sensitive nature of the information stolen. Plaintiffs face a substantial risk of out-of-pocket fraud losses, such as loans opened in their name, medical services billed in their name, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

221. Kaplan Plaintiffs will now be forced to expend additional time to freeze credit, review credit reports and monitor financial accounts and medical records for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

CLASS ACTION ALLEGATIONS

222. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

223. Plaintiffs propose the following Nationwide Class definition, subject to amendment as appropriate:

> All persons who Defendants identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

224. Plaintiffs also propose to represent a New York State Subclass defined as follows and subject to amendment as appropriate:

> All New York residents who Defendants identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of

the Data Breach.

225. The Nationwide Class and the New York Subclass are collectively referred to herein as the "Classes."

226. Excluded from the Classes are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

227. Plaintiffs reserve the right to amend or modify the Class definitions or create additional subclasses as this case progresses.

228. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over three million individuals who Private Information was compromised in the data breach.

229. **Commonality.** There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendants' data security systems prior to and during the Data Breach were

consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breached implied contracts with Plaintiffs and Class Members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

230. **Typicality.** Named Plaintiffs' claims are typical of those of other Class Members because named Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

231. **Adequacy or Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest

that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

232. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the data of Plaintiffs and Class Members was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

233. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would, therefore, have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

234. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to

the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

235. **Ascertainability & Notice.** Membership in the Class can be determined by objective records maintained by Defendant and adequate notice can be given to Class Members directly using information maintained in Defendant's records. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

236. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE
(On behalf of Plaintiffs & the Nationwide Class)

237. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

238. By collecting and storing the Private Information of Plaintiffs and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

239. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, or their third-party vendor systems and networks, and the personnel responsible for them, adequately protected the Private Information.

240. Plaintiffs and Class Members are a well-defined, foreseeable and probable group of patients that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

241. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

242. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

243. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

244. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

245. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems or ensure their third-party vendors adequately monitor the security of their systems and networks;

c. Failing to ensure that their email systems had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII and PHI, and

h. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

246. Plaintiffs and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

247. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

248. It was, therefore, foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the previous data breach at

Northwell and the known high frequency of cyberattacks and data breaches in the healthcare industry.

249. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

250. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

251. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

252. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

253. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT II

NEGLIGENCE *PER SE*
(On behalf of Plaintiffs & the Nationwide Class)

254. Plaintiffs and Class Members repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

255. In addition to the common law and special relationship duties alleged herein, Defendants also owed a duty to safeguard Plaintiffs' and Class Members' Private Information by statute.

256. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

257. Defendants failed to, or contracted with companies that failed to, use reasonable security measures under HIPAA to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

258. In addition, Defendants failed to, or contracted with companies that failed to, employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

259. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

260. Defendants breached that duty, which, as discussed herein, caused Plaintiffs and Class Members injuries, for which they are entitled to damages.

261. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injuries and are entitled to nominal, compensatory, consequential and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT III

GROSS NEGLIGENCE
(On Behalf of Plaintiffs & the Nationwide Class)

262. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

263. Defendants knew that they were protecting the most sensitive Private Information about Plaintiffs and Class Members that exists—healthcare information—which can impact anything from housing, employment, benefits, education, and other areas of an individual's life.

264. When that Private Information is compromised, the effects can be devastating to individuals, such that Defendants knew or should have known about these effects and the need to keep this information secure and protected.

265. Defendants' failure to keep this information safe was grossly negligent, as Defendants were aware of the grave consequences of not keeping this information secure.

266. As a result of Defendants' gross negligence, Plaintiffs and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT IV

BREACH OF THIRD-PARTY BENEFICIARY CONTRACTS
(On behalf of Plaintiffs & the Nationwide Class)

267. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

268. Defendants Northwell and PJ&A had valid contracts with each other, including "business associate agreements under HIPAA," for the purpose of providing medical transcription services on behalf of Northwell's patients.

269. These contracts were made expressly for Plaintiffs and the Class, as it was their confidential medical information that PJ&A agreed to collect and protect through its services.

270. The benefit of secure collection, transmission and protection of the PHI and PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

271. Plaintiffs and Class Members are also intended third-party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendants intended to give the beneficiaries the benefit of the promised performance.

272. Defendants knew that if they were to breach these contracts, Northwell's patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

273. Defendants breached their contracts when they failed to use reasonable data

security measures and allowed the Data Breach to occur, and as otherwise set forth herein.

274. Defendants' breach caused foreseeable and material damages to Plaintiffs and Class Members including but not limited to the risk of harm through the loss of their Private Information.

275. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT V

BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs & the Nationwide Class)

276. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

277. Plaintiffs bring this claim for breach of implied contract in the alternative to their breach of their-party beneficiary contract claim.

278. Defendants acquired and maintained the Private Information of Plaintiffs and the Class that they received either directly or indirectly from their patients and/or healthcare provider customers.

279. When Plaintiffs and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates and vendors, including Defendants.

280. Plaintiffs and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

281. Plaintiffs and the Class were required to deliver their Private Information to

Defendants as part of the process of obtaining services provided by Defendants. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

282. Defendants solicited, offered and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendant Northwell, or, alternatively, provided Plaintiffs' and Class Members' information to doctors or other healthcare professionals, who then provided to Defendant PJ&A.

283. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services or Plaintiffs and Class Members.

284. In accepting such information and payment for services, Defendants entered into an implied contract with Plaintiffs and the other Class Members whereby Defendants became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

285. Alternatively, Plaintiffs and Class Members were the intended beneficiaries of data protection agreements entered into between Defendants.

286. In delivering their Private Information to Defendants and paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard the data as part of that service.

287. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

288. The implied promises include but are not limited to: (1) taking steps to ensure that

any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

289. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

290. Had Defendants disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Private Information to Defendants.

291. Defendants recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

292. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Defendants.

293. Defendants breached the implied contracts with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

294. As a direct and proximate result of Defendants' conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT VI

UNJUST ENRICHMENT
(On Behalf of Plaintiffs & the Nationwide Class)

295. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

296. This count is pleaded in the alternative to all breach of contract claims, above (Counts IV-VI).

297. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from money they make based upon protecting Plaintiffs' and Class Members' Private Information.

298. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiffs' and Class Members' Private Information confidential and protected.

299. Plaintiffs and Class Members paid Defendants and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendants.

300. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

301. Protecting data from Plaintiffs and the rest of the Class Members is integral to Defendants' business. Without their data, Defendants would be unable to provide the clinical lab testing services comprising Defendants' core business.

302. Plaintiffs' and Class Members' data has monetary value, and Defendants realize this benefit when they choose to store such data.

303. Plaintiffs and Class Members directly and indirectly conferred a monetary benefit on Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods

and/or services from entities that contracted with Defendants, and from which Defendants received compensation to protect certain data. Plaintiffs and Class Members directly conferred a monetary benefit on Defendants by supplying Private Information, which has value, from which value Defendants derive their business value, and which should have been protected with adequate data security.

304. Defendants knew that Plaintiffs and Class Members conferred a benefit—which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

305. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

306. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

307. Defendants acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

308. If Plaintiffs and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants (or to their physician to provide to Defendants).

309. Plaintiffs and Class Members have no adequate remedy at law.

310. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

311. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

312. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from

them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

COUNT VII

BAILMENT
(On Behalf of Plaintiffs & the Nationwide Class)

313. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

314. Plaintiffs and Class Members provided Private Information to Defendants—either directly or through healthcare providers and their business associates—which Defendants were under a duty to keep private and confidential.

315. Plaintiffs' and Class Members' Private Information is personal property, and it was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

316. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks they took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

317. Once Defendants accepted Plaintiffs' and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

318. Defendants did not safeguard Plaintiffs' or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

319. Defendants' failure to safeguard Plaintiffs' and Class Members' Private

Information resulted in that information being accessed or obtained by third-party cybercriminals.

320. As a result of Defendants' failure to keep Plaintiffs' and Class Members' Private Information secure, Plaintiffs and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—is appropriate.

COUNT VII

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs & the Nationwide Class)

321. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

322. In light of the special relationship between Defendants and Plaintiffs and Class Members, Defendants became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure and (3) to maintain complete and accurate records of what information (and where) Defendants do store.

323. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with their patients, in particular, to keep secure their Private Information.

324. Defendants breached their fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

325. Defendants breached their fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

326. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendants' services they received.

327. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IX

BREACH OF CONFIDENCE
(On Behalf of Plaintiffs & the Nationwide Class)

328. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

329. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendants

and ultimately accessed and acquired in the Data Breach.

330. At all times during its possession and control of Plaintiffs' and Class Members' Private Information, Defendants were fully aware of the confidential, novel and sensitive nature of Plaintiffs' and Class Members' Private Information provided to it.

331. As alleged herein and above, Defendants' possession and control of Plaintiffs' and Class Members' highly sensitive Private Information was governed by the expectations of Plaintiffs and Class Members that their Private Information would be collected, stored and protected in confidence, and that it would not be disclosed to unauthorized third parties.

332. Plaintiffs and Class Members provided their respective Private Information with the understanding that it would be protected and not disseminated to any unauthorized parties.

333. Plaintiffs and Class Members also provided their respective Private Information with the understanding that precautions would be taken to protect it from unauthorized disclosure, and that these precautions would at least include basic principles of information security practices.

334. Defendants voluntarily received, in confidence, Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

335. Due to Defendants' failure to prevent, detect and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized criminal third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

336. But for Defendants' unauthorized disclosure of Plaintiffs' and Class Members' Private Information, their Private Information would not have been compromised, stolen, viewed,

accessed, and used by unauthorized third-party criminals. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

337. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendants knew or should have known that its security systems were insufficient to protect the Private Information that is coveted and misused by thieves worldwide. Defendants also failed to observe industry standard information security practices.

338. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered damages as alleged herein.

COUNT X

BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiffs & the Nationwide Class)

339. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

340. Plaintiffs and Class Members entered into valid, binding and enforceable express or implied contracts with entities affiliated with or serviced by Defendants, as alleged above.

341. The contracts respecting which Plaintiffs and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendants would act fairly and in good faith in carrying out their contractual obligations to take

reasonable measures to protect Plaintiffs' PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

342. A "special relationship" exists between Defendants and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members who sought medical services from Northwell and/or PJ&A and, in doing so, entrusted Defendants, pursuant to their requirements and Privacy Notice, with their PII and PHI.

343. Despite this special relationship with Plaintiffs, Defendants did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII and PHI.

344. Plaintiffs and Class Members performed all conditions, covenants, obligations and promises owed to Defendants.

345. Defendants' failure to act in good faith in complying with the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

346. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT XI

INVASION OF PRIVACY
(On Behalf of Plaintiffs & the Nationwide Class)

347. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

348. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendants mishandled.

349. As a result of Defendants' conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

350. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

351. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

352. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

353. Plaintiffs and Class Members are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

354. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT XII

VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT
New York General Business Law ("GBL") § 349
(On Behalf of Plaintiffs & the New York Class)

355. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

356. New York Deceptive Trade Practices Act, N.Y. Gen. Bus. Law § 349, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

357. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the N.Y. Gen. Bus. Law § 349. The conduct alleged herein is a "business practice" within the meaning of the N.Y. Gen. Bus. Law § 349, and the deception occurred within New York State.

358. Defendants stored Plaintiffs' and New York SubClass Members' Private Information in Defendants' electronic databases. Defendants knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiffs' and New York SubClass Members' Private Information secure and prevented the loss or misuse of that Private Information. Defendants did not disclose to Plaintiffs and New York SubClass Members that its data systems were not secure.

359. Plaintiffs and New York SubClass Members would not have provided their Private

Information if they had been told or knew that Defendants failed to maintain sufficient security thereof, and its inability to safely store Plaintiffs' and New York SubClass Members' Private Information.

360. As alleged herein in this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

a. Representing that their services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York SubClass Members' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York SubClass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and New York SubClass Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and New York SubClass Members' Private Information; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York SubClass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

361. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to

protect the confidentiality of consumers' Private Information.

362. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendants. These deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, N.Y. Gen. Bus. Law § 349.

363. In addition, Defendants' failure to secure patients' Private Information violated the FTCA and, therefore, violates N.Y. Gen. Bus. Law § 349.

364. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiffs and New York SubClass Members, deter hackers and detect a breach within a reasonable time, and that the risk of a data breach was highly likely. Plaintiffs and New York SubClass Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties and attorneys' fees and costs.

365. The conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

366. Defendants' violations of N.Y. Gen. Bus. Law § 349 have an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had their Private Information stored on Defendants' electronic database, many of whom have been impacted by the Data Breach.

367. As a direct and proximate result of these deceptive trade practices, Plaintiffs and New York SubClass Members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin

further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees) and such other relief as the Court deems just and proper.

368. On information and belief, Defendants formulated and conceived of the systems used to compile and maintain patient information largely within the state of New York, oversaw its data privacy program complained of herein from New York, and its communications and other efforts to hold participant data largely emanated from New York.

369. Defendants' implied and express representations that it would adequately safeguard Plaintiffs' and New York SubClass Members' Private Information constitute representations as to the particular standard, quality or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

370. Accordingly, Plaintiffs, on behalf of themselves and New York SubClass Members, bring this action under N.Y. Gen. Bus. Law § 349 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT XIII

NEW YORK CONSTITUTION RIGHT TO PRIVACY
(On Behalf of Plaintiffs & the New York Class)

371. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

372. The New York Constitution provides: "[n]o person shall be deprived of life, liberty or property without due process of law." (N.Y. Const., art. I, § 6.)

373. Plaintiffs and the New York Subclass had a legally recognized and protected privacy interest in the personal medical information provided to and obtained by Defendants,

including but not limited to an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes.

374. Plaintiffs and the New York Subclass reasonably expected Defendants would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal medical information.

375. Defendants' conduct described herein resulted in a serious invasion of the privacy of Plaintiffs and the New York Subclass, as the release of personal medical information, including but not limited to names, social security numbers, dates of medical lab testing, and medical lab test results could highly offend a reasonable individual.

376. As a direct consequence of the actions as identified above, Plaintiffs and the New York Subclass suffered harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed.

COUNT XIII

DECLARATORY & INJUNCTIVE RELIEF
(On Behalf of Plaintiffs & the Nationwide Class)

377. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

378. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*

379. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

380. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendants is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

381. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

382. Defendants still possess the Private Information of Plaintiffs and the Class.

383. To Plaintiffs' knowledge, Defendants have made no announcement that it has changed their data storage or security practices relating to the Private Information, beyond the vague claim in the Data Breach Letter that it is "[taking] steps to enhance the security of our computer systems and the data we maintain."

384. To Plaintiffs' knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Anatoli Belov, Irina Belova and Eryn Kaplan, individually and

as a natural guardian of H.M.K., a minor child, respectfully pray for judgment in their favor and against Defendants as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than fifteen years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees, as permitted by law;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs Anatoli Belov, Irina Belova and Eryn Kaplan, individually and as a natural guardian of H.M.K., a minor child, hereby demand that this matter be tried before a jury.

Date: November 17, 2023

Respectfully submitted,

s/: James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway New York, NY 10003
(212) 558-5500
jbilsborrow@weitzlux.com

David S. Almeida
New York Bar No. 3056520
Britany a. Kabakov*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
T: (312) 576-3024
E: david@almeidalawgroup.com
E: britany@almeidalawgroup.com

**Pro Hac Vice applications to be submitted*

Attorneys for Plaintiffs & Putative Classes